

From: mkmcguire@mail.ci.lubbock.tx.us
To: Jeanelle Wadkins, James Shavers, Katherine Wilkinson
CC: Mario Gonzalez, Janci Wilson, Mark Wims
Subject: RE: Open Records Request - Regarding Facial Recognition Software
Date: 2019-07-16 08:53
Attachments: RE: Open Records Request - Regarding Facial Recognition Software.html [\[Save\]](#) [\[Open\]](#)
FR Course Test_Student.pdf [\[Save\]](#) [\[Open\]](#)
Course Objectives - LPR Technology & Best Practices.pdf [\[Save\]](#) [\[Open\]](#)
Proprietary Letter - VSCRT FR.PDF [\[Save\]](#) [\[Open\]](#)
PUR-14542 Police License Plate Reader.pdf [\[Save\]](#) [\[Open\]](#)
Course Objectives -FR Technology & Best Practices.pdf [\[Save\]](#) [\[Open\]](#)
Instructor Bios 06142018.pdf [\[Save\]](#) [\[Open\]](#)
Creation Date: 2019-07-16 08:53
Store Date: 2019-07-17 19:15
Status: read
Box Type: sent
Folder: Marian McGuire > Sent Items
Message Id: 1b3eeaded8686447b288e6dfff2f276c00000000010a#1b3eeaded8686447b288e6dfff2f276c0003b8b52ff0

A text version of the message is not available. Please refer to TEXT.htm.

What exactly do you need? Someone will have to get IT to do a search of my e-mails for 'facial rec' because there are dozens (probably close to 200 between Vigilant and me for various things concerning the system plus the ones internally).

I don't know what they want concerning training. I probably have the handouts they gave us in training but I'll have to check at home. Mario may have his. I've attached the course outline & instructor bios.

I attached the agreement we have with Vigilant. Janci has the original copy.

I'm not sure what else I can provide.

From: Katherine Wilkinson
Sent: Thursday, July 11, 2019 4:43 PM
To: Jeanelle Wadkins <JWadkins@mail.ci.lubbock.tx.us>; Ray Mendoza <RMendoza@mail.ci.lubbock.tx.us>; Mario Gonzalez <MGonzalez@mail.ci.lubbock.tx.us>; Marian McGuire <mkm McGuire@mail.ci.lubbock.tx.us>; Keith Woodard <KWoodard@mail.ci.lubbock.tx.us>
Cc: Stacy Austin <StacyAustin@mail.ci.lubbock.tx.us>
Subject: Open Records Request - Regarding Facial Recognition Software

All,

We have received the attached Open Records request for records involving Facial Recognition Technology. The request covers everything from unsolicited marketing materials, meetings, emails, contracts, policies, trainings, etc. Please forward me a copy of all records(digital and print)

pertaining to any Facial Recognition Technology as soon as possible since we are on a deadline to submit to the AG. (This would include the LPR system since it has facial recognition) If you know of anyone that would have responsive documents for this ORR, please forward to them and let me know.

Thank you,

Katherine Wilkinson

Records System Manager

Lubbock Police Department

(806) 775-2805

What exactly do you need? Someone will have to get IT to do a search of my e-mails for 'facial rec' because there are dozens (probably close to 200 between Vigilant and me for various things concerning the system plus the ones internally).

I don't know what they want concerning training. I probably have the handouts they gave us in training but I'll have to check at home. Mario may have his. I've attached the course outline & instructor bios.

I attached the agreement we have with Vigilant. Janci has the original copy.

I'm not sure what else I can provide.

From: Katherine Wilkinson

Sent: Thursday, July 11, 2019 4:43 PM

To: Jeanelle Wadkins <JWadkins@mail.ci.lubbock.tx.us>; Ray Mendoza <RMendoza@mail.ci.lubbock.tx.us>; Mario Gonzalez <MGonzalez@mail.ci.lubbock.tx.us>; Marian McGuire <mkmcguire@mail.ci.lubbock.tx.us>; Keith Woodard <KWoodard@mail.ci.lubbock.tx.us>

Cc: Stacy Austin <StacyAustin@mail.ci.lubbock.tx.us>

Subject: Open Records Request - Regarding Facial Recognition Software

All,

We have received the attached Open Records request for records involving Facial Recognition Technology. The request covers everything from unsolicited marketing materials, meetings, emails, contracts, policies, trainings, etc. Please forward me a copy of all records(digital and print) pertaining to any Facial Recognition Technology as soon as possible since we are on a deadline to submit to the AG. (This would include the LPR system since it has facial recognition) If you know of anyone that would have responsive documents for this ORR, please forward to them and let me know.

Thank you,

Katherine Wilkinson

Records System Manager

Lubbock Police Department

(806) 775-2805

License Plate Recognition Technology and Best Practices Objectives

1. Attendees will be able to explain and describe the history of License Plate Recognition (LPR) technology, LPR terminology, and how the camera systems work. They will also be able to demonstrate the importance of LPR technology and data.
2. Attendees will be able to interpret key points of concern from privacy advocates, the importance of establishing general/operational orders, best practices methods, and current case law relating to LPR.
3. Attendees will be able to describe and utilize LPR Hotlists, where they are available, how best to deploy and use them, the ability to explain to their agencies how they are generated, and the different ways you can receive LPR Hotlists notifications (LPR car vs. alerts).
4. Attendees will be able to classify and describe where LPR data comes from, the different types of LPR data (Private vs. LE), available analytical resources, how to use LPR databases, how to report LPR usage, and the future of LPR data.
5. Attendees will leave feeling confident in LPR databases to find case solving leads. This will include the ability to search full or partial plates, map detections, search by Year/Make/Model, search within a geo-zone for LPR scans, create a hot plate/list, and run a full analytical report of all location, times, and dates of license plate. To do this, hand-on demos will be conducted.

Facial Recognition Technology and Best Practices Objectives

1. Attendees will explain & describe the history of Facial Recognition (FR) technology and how best it is used in accordance with existing case law by highlighting best practices. This will include the ability to understand the need to a Departmental Program Policy and different kinds of LEA FR program types.
2. Attendees will be able to identify when an agency would want to utilize FR and where it can best assist them. This will include FR in social media cases, the importance of high quality probe and mugshot images, and interpreting pose variations.
3. Attendees will be able to classify image identification, how to document the process, and the important of image enhancement when an uncontrolled image.
4. Attendees will be able to analyze and conduct the process of running the probe image within FR, identify a possible match candidate, and understand FR as a lead generation tool.
5. Attendees will be able to define the important of the "Facial Recognition Workflow" and the different aspects of a good FR software, along with listing the innovative ways FR technology is being deployed.
6. Attendees will be able to operate within FR software, that will include how to manage galleries, importing of images, use of filters, enhancement tools, and available reporting options. This will ensure the attendees can develop results using FR software.

Name: _____ Date: _____

Agency: _____

Facial Recognition Written Examination
Multiple Choice Exam:

Students will be presented with thirty (30) multiple choice questions derived from each lesson plan covered by the instructor during the course and any required reading material at the end of each lesson. Student proficiency and competency will be determined when the student achieves a minimum passing score of: (70%).

Question 1 – The facial recognition process requires a great deal of manual, human analysis and an image of a certain quality to return a possible match candidate.

- a.) True
- b.) False

Question 2 - Which of the following factors may affect facial recognition algorithms and matching accuracy?

- a) Low resolution (the number of pixels that make up the subject's face)
- b) Poor lighting leading to under or over exposure of the face
- c) Video compression whereby the recording device removes fine feature detail to save recording space
- d) All the above

Question 3 – All of the following are examples of controlled images and are considered optimal for facial recognition searching EXCEPT:

- a.) A photo of an unknown subject taken by an officer in the field to enroll into a facial recognition database
- b.) Photos captured at popular kiosk locations such as passport stations or security desks
- c.) A photo captured by video doorbell camera system which appears to have a fisheye effect
- d.) A fraudulent photo identification card left behind during the commission of a crime

Question 4 - The human element of the facial recognition process remains essential to getting a possible match and generating a valuable lead.

- a.) True
- b.) False

Question 5 – All of the following are considered best practices when a field officer conducts an image capture for the purposes of facial recognition EXCEPT:

- a.) The field officer controls the photo capture
- b.) A single field officer attempts to perform an image capture on three unknown subjects
- c.) The distance of the capture is 2-5 feet away from the subject
- d.) The subject is facing forward with eyes looking straight ahead

Question 6 - When submitting images or videos for facial recognition, the following are considered best practices when applicable EXCEPT:

- a.) Submitting original, uncropped images and videos sourced from CCTV cameras
- b.) Submitting proprietary codecs when security makes them available
- c.) Submitting a cellphone image capture of a computer screen playing a video in lieu of obtaining the original video file
- d.) Retaking an image to ensure the subject is facing forward and has little to no exaggerated facial expressions

Question 7 – All of the following statements are true regarding a face examiner's responsibility to evaluate probe images for facial recognition EXCEPT:

- a.) If the submitted image is classified by a face examiner as "controlled" it is automatically enrolled for facial recognition searching.
- b.) If the submitted image is heavily pixilated and the face examiner can see some facial definition the image meets the criteria for facial recognition searching and facial comparison
- c.) When faces in images appear skewed, distorted or fish-eyed, face examiners can correct these issues by utilizing enhancement tools
- d.) A face examiner receives an image of an unknown suspect looking directly into a camera wearing a hood and mask and classifies it as "uncontrolled"

Question 8 - To return a possible match using facial recognition, a probe image must have an associated database image.

- a.) True
- b.) False

Question 9 – A face examiner should expect an image of lower quality to return high in the candidate return list.

- a.) True
- b.) False

Question 10 – Use of filters by a face examiner during a facial recognition search do all the following EXCEPT:

- a.) Filters read the metadata attached to every image in the gallery
- b.) Filters impact matching accuracy negatively during facial recognition searches
- c.) Filters substantially drive results to levels of specificity when searching against larger databases
- d.) Filters applied to images with lower resolution increase the likelihood of obtaining a possible match

Question 11 - When the probe image is lower in quality, face examiner's need to become more actively involved in the facial identification process.

- a.) True
- b.) False

Question 12 – Which of the following statements is TRUE?

- a.) A face examiner should rely solely on the facial recognition application results
- b.) Unique identifiers such as scars, moles or piercings should be overlooked during facial comparison
- c.) During the facial identification process a face examiner looks for similarities as well as differences when comparing each face within the images
- d.) Ears are not considered important when analyzing faces

Question 13 – Once the candidate's physical characteristics have been satisfied in the facial identification process, a face examiner immediately does all the following EXCEPT:

- a.) Check for incarceration status
- b.) Hand off the selected candidate as a viable investigative lead
- c.) Conduct a complete criminal background check including modus operandi
- d.) Compare candidate's residences in relation to the location of the crime

Question 14 – Enhancement tools utilized by a face examiner during image pre-processing simply raise the probe image facial recognition quality to levels conducive for searching and yield better results.

- a.) True
- b.) False

Question 15 – The eyes are not important to the overall facial recognition process.

- a.) True
- b.) False

Question 16 – Which of the following are telltale signs of a “selfie” image?

- a.) A face examiner observes a camera flash is captured within the image
- b.) A sports emblem appears reversed on an unknown subject’s clothing
- c.) Unique identifiers such as scars, moles or tattoos appear reversed when comparing them to a likely candidate match with the same features found in list of candidates
- d.) All the above

Question 17 – When a distorted image capture sourced from an ATM machine, bank surveillance camera or other form of CCTV capture is considered for facial recognition, the next logical step the face examiner takes is the following:

- a.) Immediately enroll the distorted image into the facial recognition application and perform a search
- b.) Discard the image because it does not meet the criteria for facial recognition searching
- c.) Consider using the enhancement tools to make the face in the image appear more natural and scaled
- d.) Find five similar distorted faces from the gallery and output a photo array report

Question 18 – All are examples of images which do not meet the criteria for facial recognition searching EXCEPT:

- a.) An image that has very low lighting conditions
- b.) An image that is high with pixilation
- c.) An image with a normalized pose and good facial detail is present
- d.) An image where the subject is too far from the camera

Question 19 – Facial recognition is an absolute science comparable to DNA and Fingerprints.

- a.) True
- b.) False

Question 20 - Facial recognition technology can ONLY be used to aid in the investigation. It is not considered “sufficiently reliable to be admissible at trial”. Arrests cannot be made solely based on a facial recognition possible match. The onus still falls on the agency to establish probable cause by other investigatory means after a candidate match has been made.

- a.) True
- b.) False

Question 21 – The minimum number of candidate returns requested by a face examiner prior to the execution of a facial recognition search should be?

- a.) Top 10
- b.) Top 50
- c.) Top 100
- d.) Top 250

Question 22 - A facial recognition match is NOT the basis for arrest.

- a.) True
- b.) False

Question 23 – Which of the following is NOT considered best practice for facial recognition investigations?

- a.) Documenting image enhancements
- b.) Annotating distinguishing facial landmarks found on the probe and candidate match images
- c.) Conducting an immediate background investigation on a candidate selected from the gallery list
- d.) A face examiner draws independent conclusions without consulting peers for a secondary review

Question 24 - The goal for public safety use of facial recognition technology is to generate a strong investigative lead.

- a.) True
- b.) False

Question 25 – With regard to images of lower quality, all the following raise facial recognition matching accuracy EXCEPT:

- a.) Using enhancement tools
- b.) Narrowing the gallery size
- c.) Using descriptive filters
- d.) Outputting reports

Question 26 – There are approximately ____ facial landmarks, also known as nodal points, on a human face.

- a.) 72
- b.) 90
- c.) 100
- d.) 150

Commented [PB1]: Added commas

Commented [DR2]: Should be changed to '90'

Commented [PB3]: Duplicate questions as #27

Question 27 – During the facial comparison process, it is considered best practice for a face examiner to compare probe images and gallery images by dissecting each face into _____ quadrants.

- a.) 2
- b.) 4
- c.) 6
- d.) 8

Commented [DR4]: Incomplete question

Commented [PB5R4]: Completed sentence with email suggestions

Question 28 – All the following describe humanitarian reasons for using facial recognition EXCEPT:

- a.) Attempts to identify a deceased person with no identification
- b.) Attempts to identify lost or missing children
- c.) Attempts to identify an elderly person stricken with dementia or a homeless person with mental illness
- d.) Attempts to identify an unknown person as a favor for a work colleague

Question 29 - It is always recommended any agency electing to use facial recognition capabilities should document each search and have full auditing capabilities.

- a.) True
- b.) False

Question 30 – Which statement holds true for face annotations, landmark measurements and audit trails on all image enhancements?

- a.) They serve as evidentiary documentation for court
- b.) They highlight a historical and chronological workflow taken by the face examiner
- c.) They provide a breakdown of steps taken during forensic face comparative analysis
- d.) All of the above

END

Kyle Hoertsch
Director, Client Relations Team
SSD Detective Sergeant, Retired
Vigilant Solutions

Kyle Hoertsch retired from Sacramento County Sheriff's Department as a Detective Sergeant after a 22-year career. During that time, Kyle held assignments as a Deputy Sheriff in Corrections, Patrol, Fugitive Apprehension, Narcotics Investigations, and as an Enforcement Canine Handler. As a sergeant Kyle was assigned to Corrections, Communications, Task Force Commander for the Regional Sex Offender Task Force, Intelligence Unit and the Department's Technical Operations Unit. Since 2012, Kyle also held collateral duties as the Department's License Plate Recognition (LPR) and Facial Recognition (FR) administrator. The LPR program consisted of 40 mobile units, 50 fixed cameras, 25 custom hotlists, and over 800 users. The FR program consisted of a local gallery of 1.5 million booking images and was deployed to 557 mobile users who used IOS devices for field identifications.

In addition to his duties at the department Kyle has trained over 2000 law enforcement professionals across the United States in the use of FR and LPR. During his 22 years in LE, Kyle has always incorporated technology in his daily duties and has a wide knowledge base of technological centric enforcement tools. Kyle has been recognized as a court expert in are of LPR and has testified as such numerous times.

Roger Rodriguez
Director, Client Relations Team
NYPD Detective, Retired
Vigilant Solutions

Roger Rodriguez joined the Vigilant Solutions team after serving over twenty years with the New York City Police Department (NYPD). A former Detective and member of the NYPD Real-Time Crime Center and Intelligence Division, Roger is the one of the world's most experienced facial recognition practitioners for public safety initiatives and criminal investigations. With Vigilant, Roger is a member of various Governmental Committees in Washington DC establishing protocols and policy relating to facial recognition technology use in law enforcement. The expertise that Roger carries is unmatched in the industry. He is a practitioner and pioneer in this space having worked many criminal investigations and has offered counsel to many law enforcement agencies, biometric developers and vendors. Today, Roger drives the Facial Recognition (**FACESEARCH™**), License Plate Reader (**PLATESEARCH™**), and (**BALLISTICSEARCH™**) analytic product lines for Vigilant Solutions as Director of Client Relations, domestically and abroad. As subject matter expert and author, he shares his experiences through thought leadership presentations, media interviews, publications, and hundreds of agencies around the world benefit from them.

David Rivera
Manager, Client Relations Team
NYPD Detective 2nd Grade, Retired
Vigilant Solutions

Dave has over 20 years of law enforcement experience with the New York City Police Department (NYPD). He has also developed and honed his technical skills thru-out his career becoming instrumental in critical NYPD projects that have improved police operations and have had a direct impact on crime reduction and have provided safer communities for the residents of New York as well as the thousands of visitors.

His field experience as well as his technical background made him an instrumental part in developing the nation's first "Real-Time Crime Center". A nerve center where crime data stored in numerous NYPD systems along with public data was culled and queried to assist in investigations leading to hundreds of arrests. The RTCC's vision changed police operations from a technological standpoint and has created a baseline on how to utilize tools to dramatically reduce the time to conduct successful investigations. The RTCC has been visited by President Barack Obama as well as hundreds of dignitaries and agencies from around the world as a viable solution to their crime reduction strategies.

"My passion for law enforcement and public safety has never wavered. Coming onboard in the role of Product Manager and now Client Relations Manager, Public Safety will afford me the opportunity interact directly with our clients on products that will have an immediate impact on public safety both at a domestic and at the international level."

Dave has been conducting License Plate Recognition (LPR) and Facial Recognition (FR) Technology for over a year to agencies across the county.

Paige Burley
Manager, Client Relations Team
Former Law Enforcement Crime Analyst, Houston & Sacramento Areas
Vigilant Solutions

Paige has dual bachelor's degrees in criminology and International Studies and a Master's in International from the University of Warwick in Coventry, England. She began her career as a crime analyst at Harris County Sheriff's Office in Houston, Texas, by being one of the first analysts in their Real Time Crime Center. Shortly after, she transitioned to Houston Police Department as a Criminal Intelligence Analyst and began to focus on more long form types of analysis. Her latest LE position was a Regional Crime Analyst for the Sacramento Region, where she worked to encourage jurisdictions to communicate and link crimes that cross jurisdictional lines.

Paige has presented at numerous Crime Analyst Conferences across the country, with two being at International Association of Crime Analysts (IACA). She now works at Vigilant Solutions, helping to train LE members throughout 100's of agencies on License Plate Recognition & Facial Recognition Technology.



Training Coordinator
Lubbock County Sheriff's Office
712 Broadway St, Lubbock, TX 79401

Dear Sir or Madam,

The course listed below is presented by instructors specially trained in the topic listed below.

Course Name: Facial Recognition Technology & Best Practices
Course Hours: 8 Hours
Course Description: The Facial Recognition Technology & Best Practice course will provide an in-depth overview of the current state of Facial Recognition Technology, legal aspects, and best deployment practices. Attendees will leave feeling confident implementing facial recognition technology to generate case-solving leads.

All course material was researched and prepared by Kyle Hoertsch who is employed by Vigilant Solutions. The class is currently certified by California POST for law enforcement continued education credits.

For audit, evaluation or other reasons, TCOLE may request to review training material. Verification of course materials may be requested by contacting:

Kyle Hoertsch, Director of Client Relations Team at Vigilant Solutions
1152 Stealth St, Livermore, CA, 94551
916-606-0450
crt@vigilantsolutions.com

Sincerely,

Chris Morgan
Manager, Customer Training and Development



Enterprise Service Agreement (ESA)

This Vigilant Solutions Enterprise Service Agreement (the "Agreement") is made and entered into as of this _____ Day of _____, 201__ by and between **Vigilant Solutions, LLC**, a Delaware corporation, having its principal place of business at 1152 Stealth Street, Livermore, CA 94551 ("Vigilant") and City of Lubbock Police Department, a law enforcement agency (LEA) or other governmental agency, having its principal place of business at 916 Texas Avenue, Lubbock, Texas 79401 ("Affiliate").

WHEREAS, Vigilant designs, develops, licenses and services advanced video analysis software technologies for the law enforcement and security markets;

WHEREAS, Vigilant provides access to license plate data as a value-added component of the Vigilant law enforcement package of license plate recognition equipment and software;

WHEREAS, Affiliate will separately purchase License Plate Recognition (LPR) hardware components from Vigilant and/or its authorized reseller for use with the Software Products (as defined below);

WHEREAS, Affiliate desires to license from and receive service for the Software Products provided by Vigilant;

THEREFORE, In consideration of the mutual covenants contained herein this Agreement, Affiliate and Vigilant hereby agree as follows:

I. Definitions:

"Booking Images" refers to both LEA Booking Images and Commercial Booking Images.

"CJIS Security Policy" means the FBI CJIS Security Policy document as published by the FBI CJIS Information Security Officer.

"CLK" or "Camera License Key" means an electronic key that will permit each license of Vigilant's CarDetector brand LPR software or LineUp brand facial recognition software (one CLK per camera) to be used with other Vigilant approved and licensed LPR hardware components (i.e., cameras and other hardware components provided by Vigilant or provided by a Vigilant certified reselling partner that has authority from Vigilant to deliver such Vigilant-authorized components) and Software Products. CLKs shall be not issuable and if issued in error shall be removed and immediately rendered null and void for cameras and other hardware components that are not Vigilant-authorized cameras and other hardware components or are delivered to Affiliate by another vendor that is not a Vigilant certified reselling partner.

"Commercial Booking Images" refers to images collected by commercial sources and available on LEARN with a paid subscription.

"Commercial LPR Data" refers to LPR data collected by private sources and available on LEARN with a paid subscription.

"Criminal Justice Information Services Division" or "CJIS" means the FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJ to the FBI and to qualified law enforcement, criminal justice,



civilian, academic, employment, and licensing agencies.

"Effective Date" means sixty (60) days subsequent to the date set forth in the first paragraph of this Agreement.

"Enterprise License" means a non-exclusive, non-transferable license to install and operate the Software Products, on applicable media provided by Vigilant or Vigilant's certified reselling partners. This Enterprise Service Agreement allows Affiliate to install the Software Products on such devices, in accordance with the selected Service Package(s), and allow benefits of all rights granted hereunder this Agreement.

"LEA Booking Images" refers to images collected by LEAs and available on the Software Service for use by other LEAs. LEA Booking Images are freely available to LEAs at no cost and are governed by the contributing LEA's policies.

"LEA LPR Data" refers to LPR data collected by LEAs and available on LEARN for use by other LEAs. LEA LPR Data is freely available to LEAs at no cost and is governed by the contributing LEA's retention policy.

"Service Fee" means the amount due from Affiliate prior to the renewal of this Agreement as consideration for the continued use of the Software Products and Service Package benefits according to Section VIII of this Agreement.

"Service Package" means the Affiliate designated service option(s) which defines the extent of use of the Software Products, in conjunction with any service and/or benefits therein granted as rights hereunder this Agreement.

"Service Period" has the meaning set forth in Section III (A) of this Agreement.

"Software Products" means Vigilant's Law Enforcement & Security suite of Software Products including CarDetector, Law Enforcement Archival & Reporting Network (LEARN), PlateSearch, Mobile Companion for Smartphones, Target Alert Service (TAS) server/client alerting package, FaceSearch, LineUp, and other software applications considered by Vigilant to be applicable for the benefit of law enforcement and security practices. Software Products shall only be permitted to function on approved Vigilant cameras and other hardware components provided by Vigilant or through Vigilant certified reselling partners. Software Products shall not be permitted to operate on third-party provided or not Vigilant-authorized hardware components, and if found to be operating on third-party provided hardware components Software Products shall be promptly removed by Affiliate.

"Technical Support Agents" means Affiliate's staff person specified in the Contact Information Worksheet of this Agreement responsible for administering the Software Products and acting as Affiliate's Software Products support contact.

"User License" means a non-exclusive, non-transferable license to install and operate the Software Products, on applicable media, limited to a single licensee.

"Users" refers to individuals who are agents and/or sworn officers of the Affiliate and who are authorized by the Affiliate to access LEARN on behalf of Affiliate through login credentials provided by Affiliate.

II. Enterprise License Grant; Duplication and Distribution Rights:

Subject to the terms and conditions of this Agreement, Vigilant hereby grants Affiliate an Enterprise License to the



Software Products for the Term provided in Section III below. Except as expressly permitted by this Agreement, Affiliate or any third party acting on behalf of Affiliate shall not copy, modify, distribute, loan, lease, resell, sublicense or otherwise transfer any right in the Software Products. Except as expressly permitted by this Agreement, no other rights are granted by implication, estoppel or otherwise. Affiliate shall not eliminate, bypass, or in any way alter the copyright screen (also known as the “splash” screen) that may appear when Software Products are first started on any computer. Any use or redistribution of Software Products in a manner not explicitly stated in this Agreement, or not agreed to in writing by Vigilant, is strictly prohibited.

III. Term; Termination.

A. Term. The initial term of this Agreement is for one (1) year beginning on the Effective Date (the “Initial Term”), unless earlier terminated as provided herein. Sixty (60) days prior to the expiration of the Initial Term and each subsequent Service Period, Vigilant will provide Affiliate with an invoice for the Service Fee due for the subsequent twelve (12) month period (each such period, a “Service Period”). This Agreement and the Enterprise License granted under this Agreement will be extended for a Service Period upon Affiliate’s payment of that Service Period’s Service Fee, which is due 30 days prior to the expiration of the Initial Term or the existing Service Period, as the case may be. Pursuant to Section XIII below, Affiliate may also pay in advance for more than one Service Period.

B. Affiliate Termination. Affiliate may terminate this Agreement at any time by notifying Vigilant of the termination in writing thirty (30) days prior to the termination date and deleting all copies of the Software Products. If Affiliate terminates this Agreement prior to the end of the Initial Term, Vigilant will not refund or prorate any license fees, nor will it reduce or waive any license fees still owed to Vigilant by Affiliate. Upon termination of the Enterprise License, Affiliate shall immediately cease any further use of Software Products. Affiliate may also terminate this agreement by not paying an invoice for a subsequent year’s Service Fee within sixty (60) days of invoice issue date.

C. Vigilant Termination. Vigilant has the right to terminate this Agreement by providing thirty (30) days written notice to Affiliate. If Vigilant’s termination notice is based on an alleged breach by Affiliate, then Affiliate shall have thirty (30) days from the date of its receipt of Vigilant’s notice of termination, which shall set forth in detail Affiliate’s purported breach of this Agreement, to cure the alleged breach. If within thirty (30) days of written notice of violation from Vigilant Affiliate has not reasonably cured the described breach of this Agreement, Affiliate shall immediately discontinue all use of Software Products and certify to Vigilant that it has returned or destroyed all copies of Software Products in its possession or control. If Vigilant terminates this Agreement prior to the end of a Service Period for breach, no refund for any unused Service Fees will be provided. If Vigilant terminates this Agreement prior to the end of a Service Period for no reason, and not based on Affiliate’s failure to cure the breach of a material term or condition of this Agreement, Vigilant shall refund to Affiliate an amount calculated by multiplying the total amount of Service Fees paid by Affiliate for the then-current Service Period by the percentage resulting from dividing the number of days remaining in the then-current Service Period, by 365.

IV. Warranty and Disclaimer; Infringement Protection; Use of Software Products Interface.

A. Warranty and Disclaimer. Vigilant warrants that the Software Products will be free from all Significant Defects (as defined below) during the term of this Agreement (the “Warranty Period”). “Significant Defect” means a defect in a Software Product that impedes the primary function of the Software Product. This warranty does not include products not manufactured by Vigilant. Vigilant will repair or replace any Software Product with a Significant Defect during the Warranty Period; *provided, however*, if Vigilant cannot substantially correct a Significant Defect in a

commercially reasonable manner, Affiliate may terminate this Agreement and Vigilant shall refund to Affiliate an amount calculated by multiplying the total amount of Service Fees paid by Affiliate for the then-current Service Period by the percentage resulting from dividing the number of days remaining in the then-current Service Period, by 365. The foregoing remedies are Affiliate's exclusive remedy for defects in the Software Product. Vigilant shall not be responsible for labor charges for removal or reinstallation of defective software, charges for transportation, shipping or handling loss, unless such charges are due to Vigilant's gross negligence or intentional misconduct. Vigilant disclaims all warranties, expressed or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose. In no event shall Vigilant be liable for any damages whatsoever arising out of the use of, or inability to use, the Software Products.

B. Infringement Protection. If an infringement claim is made against Affiliate by a third-party in a court of competent jurisdiction regarding Affiliate's use of any of the Software Products, Vigilant shall indemnify Affiliate, and assume all legal responsibility and costs to contest any such claim. If Affiliate's use of any portion of the Software Products or documentation provided to Affiliate by Vigilant in connection with the Software Products is enjoined by a court of competent jurisdiction, Vigilant shall do one of the following at its option and expense within sixty (60) days of such enjoinder: (1) Procure for Affiliate the right to use such infringing portion; (2) replace such infringing portion with a non-infringing portion providing equivalent functionality; or (3) modify the infringing portion so as to eliminate the infringement while providing equivalent functionality.

C. Use of Software Products Interface. Under certain circumstances, it may be dangerous to operate a moving vehicle while attempting to operate a touch screen or laptop screen and any of their applications. It is agreed by Affiliate that Affiliate's users will be instructed to only utilize the interface to the Software Products at times when it is safe to do so. Vigilant is not liable for any accident caused by a result of distraction such as from viewing the screen while operating a moving vehicle.

V. Software Support, Warranty and Maintenance.

Affiliate will receive technical support by submitting a support ticket to Vigilant's company support website or by sending an email to Vigilant's support team. Updates, patches and bug fixes of the Software Products will be made available to Affiliate at no additional charge, although charges may be assessed if the Software Product is requested to be delivered on physical media. Vigilant will provide Software Products support to Affiliate's Technical Support Agents through e-mail, fax and telephone.

VI. Camera License Keys (CLKs).

Affiliate is entitled to use of the Software Products during the term of this Agreement to set up and install the Software Products on an unlimited number of media centers within Affiliate's agency in accordance with selected Service Options. As Affiliate installs additional units of the Software Products and connects them to LPR cameras, Affiliate is required to obtain a Camera License Key (CLK) for each camera installed and considered in active service. A CLK can be obtained by Affiliate by going to Vigilant's company support website and completing the online request form to Vigilant technical support staff. Within two (2) business days of Affiliate's application for a CLK, Affiliate's Technical Support Agent will receive the requested CLK that is set to expire on the last day of the Initial Term or the then-current Service Period, as the case may be.

VII. Ownership of Software.

A. Ownership of Software Products. The Software Products are copyrighted by Vigilant and remain the property of Vigilant. The license granted under this Agreement is not a sale of the Software Products or any copy. Affiliate owns the physical media on which the Software Products are installed, but Vigilant retains title and ownership of the Software Products and all other materials included as part of the Software Products.

B. Rights in Software Products. Vigilant represents and warrants that: (1) it has title to the Software and the authority to grant license to use the Software Products; (2) it has the corporate power and authority and the legal right to grant the licenses contemplated by this Agreement; and (3) it has not and will not enter into agreements and will not take or fail to take action that causes its legal right or ability to grant such licenses to be restricted.

VIII. Data Sharing, Access and Security.

If Affiliate is a generator as well as a consumer of LPR Data and or LEA Booking Images, Affiliate at its option may share its LEA LPR Data and or LEA Booking Images with similarly situated LEAs who contract with Vigilant to access LEARN (for example, LEAs who share LEA LPR Data with other LEAs). Vigilant will not share any LEA LPR Data or LEA Booking Images generated by the Affiliate without the permission of the Affiliate.

Vigilant has implemented procedures to allow for adherence to the FBI CJIS Security Policy. The hosting facility utilizes access control technologies that meet or exceed CJIS requirements. In addition, Vigilant has installed and configured network intrusion prevention appliances, as well as ensured that the configuration of the Microsoft environment adhere to the Windows Server Security Guide.

IX. Ownership and use of Data.

Vigilant retains all title and rights to Commercial LPR Data and all Commercial Booking Images. Users shall not utilize Commercial LPR Data or Commercial Booking Images on the behalf of other local, state or Federal LEAs. Affiliate retains all rights to LEA LPR Data and LEA Booking Images generated by the Affiliate. Should Affiliate terminate agreement with Vigilant, a copy of all LEA LPR Data and LEA Booking Images generated by the Affiliate will be created and provided to the Affiliate. After the copy is created, all LEA LPR Data and LEA Booking Images generated by the Affiliate will be deleted from LEARN at the written request of an authorized representative of the Affiliate or per the Affiliate's designated retention policy, whichever occurs first. Commercial LPR Data, Commercial Booking Images, LEA LPR Data and LEA Booking Images should be used by the Affiliate for law enforcement purposes only.

X. Loss of Data, Irregularities and Recovery.

Vigilant places imperative priority on supporting and maintaining data center integrity. Using redundant disk arrays, there is a virtual guarantee that any hard disk failure will not result in the corruption or loss of the valuable LPR data that is essential to the LEARN system and clients.

XI. Data Retention and Redundancy.

LEA LPR Data and LEA Booking Images are governed by the contributing LEA's retention policy. LEA LPR Data that reaches its expiration date will be deleted from LEARN. Vigilant's use of redundant power sources, fiber connectivity and disk arrays ensure no less than 99% uptime of the LEARN LPR database server system.



XII. Account Access.

A. Eligibility. Affiliate shall only authorize individuals who satisfy the eligibility requirements of "Users" to access LEARN. Vigilant in its sole discretion may deny access to LEARN to any individual based on such person's failure to satisfy such eligibility requirements. User logins are restricted to agents and sworn officers of the Affiliate. No User logins may be provided to agents or officers of other local, state, or Federal LEAs without the express written consent of Vigilant.

B. Security. Affiliate shall be responsible for assigning an Agency Manager who in turn will be responsible for assigning to each of Affiliate's Users a username and password (one per user account). A limited number of User accounts is provided. Affiliate will cause the Users to maintain username and password credentials confidential and will prevent use of such username and password credentials by any unauthorized person(s). Affiliate shall notify Vigilant immediately if Affiliate believes the password of any of its Users has, or may have, been obtained or used by any unauthorized person(s). In addition, Affiliate must notify Vigilant immediately if Affiliate becomes aware of any other breach or attempted breach of the security of any of its Users' accounts.

C. CJIS Requirements. Affiliate certifies that its LEARN users shall comply with the CJIS requirements outlined in Exhibit B.

XIII. Service Package, Fees and Payment Provisions.

A. Service Package. This Enterprise License Agreement is based on one (1) of the three (3) following Service Package Options. Please select one (1) Service Package below:

☐

Service Package - Basic LPR Service Package:

- Vigilant Managed/Hosted LPR server LEARN Account
- Access to all Vigilant Software including all upgrades and updates
- Unlimited user licensing for the following applications:
 - LEARN, CarDetector and TAS

☐

Service Package - Option # 1 – Standard LPR Service Package:

- All Basic Service Package benefits
- Unlimited use of CarDetector – Mobile Hit Hunter (CDMS-MHH)
- Unlimited use of Vigilant's LPR Mobile Companion smartphone application

☒

Service Package - Option # 2 – 'Intelligence-Led Policing (ILP)' Service Package:

- All Service Package Option # 1 benefits
- Mobile LPR hardware up to level of Tier (see Exhibit A)
- Use of Vigilant Facial Recognition technologies up to level of Tier
 - FaceSearch Account
 - FaceSearch Mobile Companion
- Templates up to limit for FaceSearch Account (details in Exhibit A)



- Tiered based on size of department (Tier 1A up to 50 sworn officers Tier 1 up to 100 sworn officers, Tier 2 up to 200 sworn officers, Tier 3 up to 500 sworn officers, Tier 4 up to 1,000 sworn officers, Tier 5 up to 1,500 sworn officers, Tier 6 up to 2,000 sworn officers)
- States, Federal Agencies, and Departments with greater than 2,000 sworn fall under a, "Custom" Tier which will be defined in the Annual Service Fee Schedule if applicable.

B. Service Fee. Payment of each Service Fee entitles Affiliate to all rights granted under this Agreement, including without limitation, use of the Software Products for the relevant Service Period, replacement of CLKs, and access to the updates and releases of the Software Products and associated equipment driver software to allow the Software Products to remain current and enable the best possible performance. The annual Service Fee due for a particular Service Period is based on the number of current Vigilant issued CLK's at the time of Service Fee invoicing, and which will be used by Affiliate in the upcoming Service Period. A schedule of annual Service Fees is shown below:

Annual Service Fee Schedule (multiplied by number of CLK's Issued)					
	Total # of CLK's under this ESA	0-14 CLK's	15-30 CLK's	31-60 CLK's	Over 60
	Basic Service	\$525.00	\$450.00	\$400.00	\$275.00
	Standard (Option # 1)	\$750.00	\$640.00	\$565.00	\$390.00
	ILP Subscriber CLK Renewal Fees	\$525.00	\$450.00	\$400.00	\$275.00

Annual Parking Fee Schedule		
	Parking Enforcement System Toolkit	\$1,000.00 per system
	Parking Integration	\$1,000.00
	Scofflaw Alerting Service	\$25,000.00

Intelligence-Led Policing Service Package Annual Fee Schedule		
	Tier	ILP Annual Fee
	ILP Tier 1 (Option #2)	\$14,995.00
	ILP Tier 2 (Option #2)	\$34,495.00
	ILP Tier 3 (Option #2)	\$59,995.00
	ILP Tier 4 (Option #2)	\$89,995.00
	ILP Tier 5 (Options #2)	\$119,995.00
	ILP Tier 6 (Option #2)	\$154,995.00

Annual Service Fee Schedule for Image Enrollment (applicable to FaceSearch/LineUp)		
	5,000 Images	\$750.00



Payment of the Service Fee is due thirty (30) days prior to the renewal of the then-current Service Period. All Service Fees are exclusive of any sales, use, value-added or other federal, state or local taxes (excluding taxes based on Vigilant's net income) and Affiliate agrees to pay any such tax. Service Fees may increase by no higher than 4% per year for years after the first year of this agreement. For LLP (Option # 2) Tier packages, the Tier amount is due for subsequent periods and Basic Service CLK fees are due for all cameras from previous periods (this is in addition to the Annual Subscription Fee).

Affiliate and Vigilant agree that the number of CLKs issued as of the Effective Date of this Agreement is ____ [Insert Quantity]. All future additions of CLKs shall only be those as provided for in the definitions provided above.

C. Advanced Service Fee Payments. Vigilant will accept advanced Service Fee payments on a case by case basis for Affiliates who wish to lock in the Service Fee rates for subsequent periods at the rates currently in effect, as listed in the table above. If Affiliate makes advanced Service Fee payments to Vigilant, advanced payments to Vigilant will be applied in full to each subsequent Service Period's Service Fees until the balance of the credits is reduced to a zero balance. System based advanced credits shall be applied to subsequent Service Fees in the amount that entities Affiliate continued operation of the designated camera unit systems for the following Service Period until the credits are reduced to a zero balance.

D. Price Adjustment. Vigilant has the right to increase or decrease the annual Service Fee from one Service Period to another; *provided, however*, that in no event will a Service Fee be increased by more than 4% of the prior Service Period's Service Fees. If Vigilant intends to adjust the Service Fee for a subsequent Service Period, it must give Affiliate notice of the proposed increase on or before the date that Vigilant invoices Affiliate for the upcoming Service Period.

XIV. Miscellaneous.

A. Limitation of Liability. IN NO EVENT SHALL VIGILANT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL DAMAGES INCLUDING DAMAGES FOR LOSS OF USE, DATA OR PROFIT, ARISING OUT OF OR CONNECTED WITH THE USE OF THE SOFTWARE PRODUCTS, WHETHER BASED ON CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE, EVEN IF VIGILANT HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. IN NO EVENT WILL VIGILANT'S LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE FEES PAID BY AFFILIATE TO VIGILANT FOR THE SOFTWARE PRODUCTS LICENSED UNDER THIS AGREEMENT.

B. Confidentiality. Affiliate acknowledges that Software Products contain valuable and proprietary information of Vigilant and Affiliate will not disassemble, decompile or reverse engineer any Software Products to gain access to confidential information of Vigilant.

C. Assignment. Neither Vigilant nor Affiliate is permitted to assign this Agreement without the prior written consent of the other party. Any attempted assignment without written consent is void.

D. Amendment; Choice of Law. No amendment or modification of this Agreement shall be effective unless in writing and signed by authorized representatives of the parties. This Agreement shall be governed by the laws of the state of California without regard to its conflicts of law.

E. Complete Agreement. This Agreement constitutes the final and complete agreement between the parties with respect to the subject matter hereof, and supersedes any prior or contemporaneous agreements, written or oral, with respect to such subject matter.

F. Relationship. The relationship created hereby is that of contractor and customer and of licensor and Affiliate. Nothing herein shall be construed to create a partnership, joint venture, or agency relationship between the parties hereto. Neither party shall have any authority to enter into agreements of any kind on behalf of the other and shall have no power or authority to bind or obligate the other in any manner to any third party. The employees or agents of one party shall not be deemed or construed to be the employees or agents of the other party for any purpose whatsoever. Each party hereto represents that it is acting on its own behalf and is not acting as an agent for or on behalf of any third party.

G. No Rights in Third Parties. This agreement is entered into for the sole benefit of Vigilant and Affiliate and their permitted successors, executors, representatives, administrators and assigns. Nothing in this Agreement shall be construed as giving any benefits, rights, remedies or claims to any other person, firm, corporation or other entity, including, without limitation, the general public or any member thereof, or to authorize anyone not a party to this Agreement to maintain a suit for personal injuries, property damage, or any other relief in law or equity in connection with this Agreement.

H. Construction. The headings used in this Agreement are for convenience and ease of reference only, and do not define, limit, augment, or describe the scope, content or intent of this Agreement. Any term referencing time, days or period for performance shall be deemed calendar days and not business days, unless otherwise expressly provided herein.

I. Severability. If any provision of this Agreement shall for any reason be held to be invalid, illegal, unenforceable, or in conflict with any law of a federal, state, or local government having jurisdiction over this Agreement, such provision shall be construed so as to make it enforceable to the greatest extent permitted, such provision shall remain in effect to the greatest extent permitted and the remaining provisions of this Agreement shall remain in full force and effect.

J. Federal Government. Any use, copy or disclosure of Software Products by the U.S. Government is subject to restrictions as set forth in this Agreement and as provided by DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013(c)(1)(ii) (Oct 1988), FAR 12.212(a)(1995), FAR 52.227-19, or FAR 52.227 (ALT III), as applicable.

K. Right to Audit. Affiliate, upon thirty (30) days advanced written request to Vigilant, shall have the right to investigate, examine, and audit any and all necessary non-financial books, papers, documents, records and personnel that pertain to this Agreement and any other Sub Agreements.

L. Notices; Authorized Representatives; Technical Support Agents. All notices, requests, demands, or other communications required or permitted to be given hereunder must be in writing and must be addressed to the parties at their respective addresses set forth below and shall be deemed to have been duly given when (a) delivered in person; (b) sent by facsimile transmission indicating receipt at the facsimile number where sent; (c) one (1) business day after being deposited with a reputable overnight air courier service; or (d) three (3) business days after being deposited with the United States Postal Service, for delivery by certified or registered mail, postage pre-paid and return receipt requested. All notices and communications regarding default or termination of this Agreement shall be



delivered by hand or sent by certified mail, postage pre-paid and return receipt requested. Either party may from time to time change the notice address set forth below by delivering 30 days advance notice to the other party in accordance with this section setting forth the new address and the date on which it will become effective.

Vigilant Solutions, LLC Attn: Sales Administration 1152 Stealth Street Livermore, CA 94551	Affiliate: <u>City of Lubbock</u> Attn: <u>Police Department</u> Address: <u>916 Texas Avenue</u> <u>Lubbock, Texas 79401</u>
--	---

M. Authorized Representatives; Technical Support Agents. Affiliate's Authorized Representatives and its Technical Support Agents are set forth below in the Contact Information Worksheet. Affiliate's Authorized Representative is responsible for administering this Agreement and Affiliate's Technical Support Agents are responsible for administering the Software Products and acting as Affiliate's Software Products support contact. Either party may from time to time change its Authorized Representative, and Affiliate may from time to time change its Technical Support Agents, in each case, by delivering 30 days advance notice to the other party in accordance with the notice provisions of this Agreement.

N. Facial Recognition Image Integration. Affiliate may elect, at its sole discretion, to have Vigilant enable the ability for the Affiliate's existing facial recognition images to be imported into its FaceSearch gallery. This process requires some reformatting of the data for compatibility. The data remains property of the Affiliate, is maintained according to the retention policy set by the Affiliate and is shared to other agencies under the rules defined by the Affiliate. This service is at an additional cost. Vigilant uses a third-party service from The Center for Law Enforcement Technology, Training, & Research, Inc. (LETR) to deliver this service. If the Affiliate elects to use this service, it acknowledges that The Center for Law Enforcement Technology, Training, & Research, Inc. a non-profit, 501(c)(3) corporation, working under contract with Vigilant and acting on behalf of the Affiliate, will perform the described services for law enforcement information sharing purposes.



IN WITNESS WHEREOF, the parties have executed the Agreement as of the Effective Date.

Manufacturer: Vigilant Solutions, LLC

Authorized Agent: Bill Quinlan

Title: Vice President Sales Operations

Date: _____

Signature: _____

Affiliate Organization: City of Lubbock

Authorized Agent: Daniel M. Pope

Title: Mayor

Date: _____

Signature: _____

ATTEST:

Rebecca Garza, City Secretary

APPROVED AS TO CONTENT:

Gregory W. Stevens, Chief of Police

APPROVED AS TO FORM:

Jeff Hartsell, Deputy City Attorney



Enterprise Service Agreement

Contact Information Worksheet

Please complete the following contact information for your Vigilant Solutions Enterprise License program.

Enterprise License Agreement Holder			
Company / Agency Name:		City of Lubbock Police Department	
Company / Agency Type:		Law Enforcement Agency	
Address:		Mailing: PO Box 2000, Lubbock, Texas 79457	
		Physical: 916 Texas Avenue, Lubbock, Texas 79401	
Primary Contact			
Name:		Marian McGuire	
Title:		Sergeant	Phone: 806-775-972
Email:		mkmcguire@mylubbock.us	
Supervisor Information			
Name:		James Shavers	
Title:		Deputy Chief	Phone: 806-775-2766
Email:		jshavers@mylubbock.us	
Financial Contact (Accounts Payable)			
Name:		Linda Cuellar	
Title:		Director of Accounting	Phone: 806-775-3253
Email:		lcuellar@mylubbock.us	
Technical Support Contact # 1			
Name:		Marian McGuire	
Title:		Sergeant	Phone: 806-775-2792
Email:		mkmcguire@mylubbock.us	
Technical Support Contact # 2			
Name:			
Title:			Phone:
Email:			

For questions or concerns, please contact Vigilant Solutions' sales team:

sales@vigilantsolutions.com

1-925-398-2079

Exhibit A: Option # 2 ILP Tier Package Components

Item Description	
ILP Bundle for Agencies of Up to 100 Sworn Includes: - Agency license for LEARN Saas - Unlimited access to Commercial LPR data - One (1) 3-Camera Mobile LPR System - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 5,000 images	
ILP Bundle for Agencies of 101 to 200 Sworn Includes: - Agency license for LEARN Saas - Unlimited access to Commercial LPR data - Two (2) 3-Camera Mobile LPR Systems - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 20,000 images	
ILP Bundle for Agencies of 201 to 500 Sworn Includes: - Agency license for LEARN Saas - Unlimited access to Commercial LPR data - Three (3) 3-Camera Mobile LPR Systems - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 50,000 images	
ILP Bundle for Agencies of 501 to 1,000 Sworn Includes: - Agency license for LEARN Saas - Unlimited access to Commercial LPR data - Four (4) 3-Camera Mobile LPR Systems - First year of Basic and Standard Service Packages - LEARN-Mobile Companion - Mobile Hit Hunter - Agency license for FaceSearch - Image gallery up to 75,000 images	

ILP Bundle for Agencies of 1,001 to 1,500 Sworn**Includes:**

- Agency license for LEARN Saas
- Unlimited access to Commercial LPR data
- Four (4) 3-Camera Mobile LPR Systems
- First year of Basic and Standard Service Packages
- LEARN-Mobile Companion
- Mobile Hit Hunter
- Agency license for FaceSearch
- Image gallery up to 100,000 images

ILP Bundle for Agencies of 1,501 to 2,000 Sworn**Includes:**

- Agency license for LEARN Saas
- Unlimited access to Commercial LPR data
- Five (5) 3-Camera Mobile LPR Systems
- First year of Basic and Standard Service Packages
- LEARN-Mobile Companion
- Mobile Hit Hunter
- Agency license for FaceSearch
- Image gallery up to 200,000 images



Exhibit B: CJS Requirements

Vigilant and the Affiliate agree on the importance of data security, integrity and system availability and that these security objectives will only be achieved through shared responsibility. Vigilant and the Affiliate agree they will more likely be successful with information security by use of the Vigilant supplied technical controls and client Affiliate use of those controls; in conjunction with agency and personnel policies to protect the systems, data and privacy.

Vigilant and the Affiliate agree that Affiliate owned and FBI-CJIS supplied data in Vigilant systems does not meet the definition of FBI-CJIS provided Criminal Justice Information (CJI). Regardless, Vigilant agrees to treat the Affiliate-supplied information in Vigilant systems as CJI. Vigilant will strive to meet those technical and administrative controls; ensuring the tools are in place for the proper protection of systems, information and privacy of individuals to the greatest degree possible.

Vigilant and the Affiliate agree that information obtained or incorporated into Vigilant systems may be associated with records that are sensitive in nature having, tactical, investigative and Personally Identifiable Information. As such, that information will be treated in accordance with applicable laws, policies and regulations governing protection and privacy of this type of data.

Vigilant and the Affiliate agree that products and services offered by Vigilant are merely an investigative tool to aid the client in the course of their duties and that Vigilant make no claims that direct actions be initiated based solely upon the information responses or analytical results. Further, Vigilant and the Affiliate agree that the Affiliate is ultimately responsible for taking the appropriate actions from results, hits, etc. generated by Vigilant products and require ongoing training, human evaluation, verifying the accuracy and currency of the information, and appropriate analysis prior to taking any action.

As such, the parties agree to do the following:

Vigilant:

1. Vigilant has established the use of FBI-CJIS Security Policy as guidance for implementing technical security controls in an effort to meet or exceed those Policy requirements.
2. Vigilant agrees to appoint a CJS Information Security Officer to act as a conduit to the client Contracting Government Agency, Agency Coordinator, to receive any security policy information and disseminate to the appropriate staff.
3. Vigilant agrees to adhere to FBI-CJIS Security Policy Awareness Training and Personnel Screening standards as required by the Affiliate.
4. Vigilant agrees, by default, to classify all client supplied data and information related to client owned infrastructure, information systems or communications systems as "Criminal Justice Data". All client information will be treated at the highest level of confidentiality by all Vigilant staff and authorized partners. Vigilant has supporting guidance/policies for staff handling the full life cycle of information in physical or electronic form and has accompanying disciplinary procedures for unauthorized access, misuse or mishandling of that information.
5. Vigilant will not engage in data mining, commercial sale, unauthorized access and/or use of any of Affiliate owned data.
6. Vigilant and partners agree to use their formal cyber Incident Response Plan if such event occurs.



7. Vigilant agrees to immediately inform Affiliate of any cyber incident or data breach, to include DDoS, Malware, Virus, etc. that may impact or harm client data, systems or operations so proper analysis can be performed and client Incident Response Procedures can be initiated.
8. Vigilant will only allow authorized support staff to access the Affiliate's account or Affiliate data in support of Affiliate as permitted by the terms of contracts.
9. Vigilant agrees to use training, policy and procedures to ensure support staff use proper handling, processing, storing, and communication protocols for Affiliate data.
10. Vigilant agrees to protect client systems and data by monitoring and auditing staff user activity to ensure that it is only within the purview of system application development, system maintenance or the support roles assigned.
11. Vigilant agrees to inform the Affiliate of any unauthorized, inappropriate use of data or systems.
12. Vigilant will design software applications to facilitate FBI-CJIS compliant information handling, processing, storing, and communication of Affiliate.
13. Vigilant will advise Affiliate when any software application or equipment technical controls are not consistent with meeting FBI-CJIS Policy criteria for analysis and due consideration.
14. Vigilant agrees to use the existing Change Management process to sufficiently plan for system or software changes and updates with Rollback Plans.
15. Vigilant agrees to provide technical security controls that only permit authorized user access to Affiliate owned data and Vigilant systems as intended by the Affiliate and data owners.
16. Vigilant agrees to meet or exceed the FBI-CJIS Security Policy complex password construction and change rules.
17. Vigilant will only provide access to Vigilant systems and Affiliate owned information through Affiliate managed role-based access and applied sharing rules configured by the Affiliate.
18. Vigilant agrees to provide technical controls with additional levels of user Advanced Authentication in Physically Non-Secure Locations.
19. Vigilant agrees to provide compliant FIPS 140-2 Certified 128-bit encryption to Affiliate owned data during transport and storage ("data at rest") while in the custody and control of Vigilant.
20. Vigilant agrees to provide firewalls and virus protection to protect networks, storage devices and data.
21. Vigilant agrees to execute archival, purges and/or deletion of data as configured by the data owner.
22. Vigilant agrees to provide auditing and alerting tools within the software applications so Affiliate can monitor access and activity of Vigilant support staff and Affiliate users for unauthorized access, disclosure, alteration or misuse of Affiliate owned data. (Vigilant support staff will only have access when granted by the Affiliate.)
23. Vigilant will only perform direct support remote access to Affiliate systems/infrastructure when requested, authorized and physically granted access to the applications/systems by the Affiliate. This activity will be documented by both parties.
24. Vigilant creates and retains activity transaction logs to enable auditing by the Affiliate data owners and Vigilant staff.
25. Vigilant agrees to provide physical protection for the equipment-storing Affiliate data along with additional technical controls to protect physical and logical access to systems and data.
26. Vigilant agrees to participate in any Information or Technical Security Compliance Audit performed by the Affiliate, state CJS System Agency or FBI-CJIS Division.
27. Vigilant agrees to perform independent employment background screening for its' staff and participate in additional fingerprint background screening as required by Affiliate.
28. Vigilant agrees that the Affiliate owns all Affiliate contributed data to include "hot-lists", scans, user information etc., is only shared as designated by the client and remains the responsibility and property of the Affiliate.



Affiliate:

1. Affiliate agrees to appoint an Agency Coordinator as a central Point of Contact for all FBI-CJIS Security Policy related matters and to assign staff that are familiar with the contents of the FBI-CJIS Security Policy.
2. Affiliate agrees to have the Agency Coordinator provide timely updates with specific information regarding any new FBI-CJIS, state or local information security policy requirements that may impact Vigilant compliance or system/application development and, to facilitate obtaining certifications, training, and fingerprint-based background checks as required.
3. Affiliate agrees to inform Vigilant when any FBI-CJIS Security Awareness Training, personnel background screening or execution of FBI-CJIS Security Addendum Certifications are required.
4. Affiliate agrees to immediately inform Vigilant of any relevant data breach or cyber incident, to include DDoS, Malware, Virus, etc. that may impact or harm Vigilant systems, operations, business partners and/or other Affiliates, so proper analysis can be performed, and Incident Response Procedures can be initiated.
5. Affiliate agrees that they are responsible for the legality and compliance of information recorded, submitted or placed in Vigilant systems and use of that data.
6. Affiliate agrees that they are responsible for proper equipment operation and placement of equipment.
7. Affiliate agrees that they are responsible for vetting authorized user access to Vigilant systems with due consideration of providing potential access to non-Affiliate information.
8. Affiliate agrees that responsibility and control of persons granted access to purchased Vigilant systems, along with data stored and transmitted via Vigilant systems, is that of the Affiliate.
9. Affiliate agrees that they have responsibility for all data security, handling and data protection strategies from point of acquisition, during transport and until submission ("Hotlist upload") into Vigilant systems.
10. Affiliate agrees to reinforce client staff policies and procedures for secure storage and protection of Vigilant system passwords.
11. Affiliate agrees to reinforce client staff policies for creating user accounts with only government domain email addresses. Exceptions will be granted in writing.
12. Affiliate agrees to reinforce client staff policies for not sharing user accounts.
13. Affiliate agrees to use Vigilant role-based access as designed to foster system security and integrity.
14. Affiliate agrees that they control, and are responsible for, appropriate use and data storage policies as well as procedures for the data maintained outside the Vigilant systems. This includes when any information is disseminated, extracted or exported out of Vigilant systems.
15. Affiliate agrees that they control and are responsible for developing policies, procedures and enforcement for applying deletion/purging and dissemination rules to information within and outside the Vigilant systems.
16. Affiliate agrees that it is their responsibility to ensure data and system protection strategies are accomplished through the tools provided by Vigilant for account and user management features along with audit and alert threshold features.
17. Affiliate agrees to use the "virtual escorting" security tools provided for managing client system remote access and monitor Vigilant support staff when authorized to assist the client.
18. Affiliate agrees that the Vigilant designed technical controls and tools will only be effective in conjunction with Affiliate created policies and procedures that guide user access and appropriate use of the system.
19. Affiliate agrees that information and services provided through Vigilant products do not provide any actionable information, Affiliate users are responsible for the validity and accuracy of their data and developing procedures to verify information with the record owner and other systems (NCIC) based upon the potential lead generated.